(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 786 973**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 15377**

(51) Int Cl[7] : **H 04 N 7/10**, H 04 N 7/167, H 04 L 9/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 04.12.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 09.06.00 Bulletin 00/23.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *INNOVATRON SA Société anonyme* — FR.

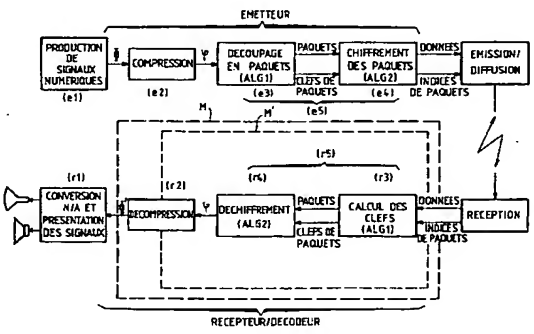
(72) **Inventeur(s)** : GRIEU FRANCOIS et MORENO ROLAND.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : CABINET BARDEHLE PAGENBERG ET PARTNER.

(54) DISPOSITIF SECURITE DECODEUR D'INFORMATIONS CHIFFREES ET COMPRIMEES, NOTAMMENT D'INFORMATIONS VIDEO, AUDIO OU DE TEXTE.

(57) Un boîtier coopère avec un microcircuit sécurisé comportant une mémoire et un processeur protégés. Le dispositif comporte: des moyens de réception de données chiffrées et comprimées; des moyens de déchiffrement (r5; r3, r4) des données reçues; des moyens de décompression (r2) des données déchiffrées; et des moyens de délivrance (r1), sous une forme décodée exploitable par un utilisateur, des données déchiffrées et décomprimées. Le microcircuit sécurisé (M; M') incorpore l'ensemble des moyens de déchiffrement (r5; r3, r4) et au moins une partie des moyens de décompression (r2), le flux (ϕ) de données déchiffrées et comprimées délivré par les moyens de déchiffrement aux moyens de décompression n'étant pas accessible depuis l'extérieur du microcircuit sécurisé. Le microcircuit sécurisé peut notamment être celui d'une carte distincte du boîtier, la liaison entre microcircuit et boîtier étant une liaison de type série utilisant au moins l'un des contacts RFU selon ISO 7816-2 pour délivrer le flux de données déchiffrées et partiellement ou totalement décompressées.



FR 2 786 973 - A1

La présente invention concerne les systèmes de diffusion d'information dans lesquels l'information est acheminée d'un diffuseur à un utilisateur sous forme comprimée et chiffrée, et dans lesquels l'utilisateur dispose d'un décodeur associé à un microcircuit électronique protégé, par exemple une carte à microcircuit, qui constitue la clef nécessaire pour que le décodeur puisse restituer une information en clair.

Les informations diffusées par de tels systèmes peuvent être variées, par exemple des signaux audio (musique) ou vidéo (programmes de télévision), ou encore des données textuelles telles que des dépêches d'agence ou des informations financières.

Le but du chiffrement est de réserver l'accès en clair de ces informations à des personnes autorisées en contrepartie d'un paiement tel qu'un abonnement ou un paiement à la séance.

Le microcircuit électronique permettant au décodeur d'assurer le déchiffrement est en général protégé contre la lecture de son contenu et contre la recopie, qu'il s'agisse d'une carte à microcircuit introduite dans un connecteur du décodeur, ou d'un microcircuit interne au décodeur.

Ce degré de sécurité n'empêche cependant pas que les informations une fois décodées puissent être copiées, permettant ainsi à l'utilisateur autorisé de faire partager la diffusion de l'information à d'autres personnes non autorisées, c'est-à-dire sans souscription d'abonnement auprès du diffuseur ou sans paiement en contrepartie de la restitution en clair de l'information.

Il existe en effet de nombreuses attaques possibles des systèmes existants dans le but d'enregistrer l'information sous une forme exploitable. Ces attaques, qui sont bien connues sur les systèmes de télédiffusion cryptée, seront explicitées dans la description détaillée qui suivra.

L'un des buts de l'invention est d'empêcher, dans la mesure du possible, que les informations une fois décodées puissent être copiées, ou tout au moins de faire en sorte que cette copie s'accompagne d'une dégradation notable de la qualité de l'information ou d'une augmentation considérable du volume des données empêchant ou rendant difficile leur enregistrement.

Essentiellement, l'invention propose à cet effet un dispositif décodeur d'informations chiffrées et comprimées, notamment d'informations vidéo, au-

dio ou de texte, du type générique connu comprenant un boîtier coopérant avec un microcircuit sécurisé comportant une mémoire et un processeur protégés à l'encontre des tentatives d'analyse et de lecture et de recopie des informations conservées dans ce microcircuit, ce dispositif décodeur comportant : des moyens de réception en entrée de données chiffrées et comprimées ; des moyens de déchiffrement des données ainsi reçues ; des moyens de décompression des données ainsi déchiffrées ; et des moyens de délivrance en sortie, sous une forme décodée exploitable par un utilisateur, des données déchiffrées et décomprimées.

Selon l'invention, le microcircuit sécurisé incorpore l'ensemble des moyens de déchiffrement et au moins une partie des moyens de décompression, le flux de données déchiffrées et comprimées délivré par les moyens de déchiffrement aux moyens de décompression n'étant pas accessible depuis l'extérieur du microcircuit sécurisé.

Le microcircuit sécurisé peut être celui d'une carte à microcircuit distincte du boîtier, ce dernier comportant des moyens de connexion permettant d'y coupler la carte à microcircuit, ou bien un microcircuit interne au boîtier.

Dans le cas d'une carte à microcircuit, la liaison entre le microcircuit et le boîtier est avantageusement une liaison de type série, très avantageusement une liaison telle que le flux de données déchiffrées et partiellement ou totalement décompressées est délivré par le microcircuit sur au moins l'un des contacts RFU selon ISO 7816-2.

Selon d'autres caractéristiques subsidiaires avantageuses :

- le boîtier comporte une partie des moyens de décompression, cette partie incluant des circuits propres à délivrer les données décomprimées en réponse à des commandes délivrées par le microcircuit sécurisé ;
- le microcircuit sécurisé inclut en outre une partie des moyens de délivrance en sortie des données sous une forme décodée exploitable, cette partie incluant notamment des moyens de traitement ou de filtrage numériques ;
- les données reçues en entrée le sont sous forme de paquets accompagnés de données associées, et les moyens de déchiffrement opèrent par mise en œuvre d'un premier algorithme permettant le calcul de clefs de paquet à partir desdites informations associées, et d'un

deuxième algorithme reconstituant un flux d'informations déchiffrées à partir des paquets et des clefs de paquet calculés par le premier algorithme ;

- le dispositif comprend des moyens de paiement conditionnant la délivrance en sortie des données sous une forme décodée exploitable à la vérification, par le microcircuit, de la réalisation préalable d'un payement en fonction d'informations tarifaires associées contenues dans une mémoire, notamment d'informations tarifaires comportant une information d'identification d'utilisateur contenue dans une mémoire du microcircuit sécurisé ;
- le dispositif comprend des moyens d'enregistrement ou des moyens de couplage à des moyens d'enregistrement, pouvant en particulier enregistrer des données comprimées et chiffrées.

◊

On va maintenant donner un exemple de mise en œuvre de l'invention, en référence aux dessins annexés.

La figure 1 est une illustration, sous forme de schéma par blocs, de la chaîne d'émission et de réception des informations, explicitant les diverses étapes de transformation des signaux.

La figure 2 représente le décodeur de l'utilisateur avec ses différents éléments associés.

La figure 3 montre les différentes plages de contact normalisées d'une carte à microcircuit.

◊

On va tout d'abord exposer en référence à la figure 1 la manière dont fonctionnent les meilleurs systèmes actuels (c'est-à-dire ceux procurant la sécurité la plus élevée à l'encontre des fraudes) de diffusion d'informations cryptées, typiquement des signaux de télévision cryptés.

On va tout d'abord décrire les étapes mises en œuvre côté émetteur :

e1) On produit tout d'abord un flux de signaux numériques, soit directement soit par numérisation de signaux analogiques, donnant ain-

si un flux de données non comprimées Φ de grand débit, de l'ordre de 10^6 bps (bits par seconde) pour l'audio et 10^8 bps pour la vidéo.

e2) Le flux Φ est ensuite comprimé selon une technique de compression avec perte d'information, par exemple du type MPEG, pour donner un flux de moyen débit ϕ, de l'ordre de 10^5 bps pour l'audio et 3.10^6 bps pour la vidéo ; cette opération met en œuvre des moyens techniques relativement évolués, c'est-à-dire nécessitant une forte puissance de calcul, pour parvenir à une compression qui n'altère pas trop la qualité sonore ou visuelle du signal;

e3) Ce flux comprimé ϕ est ensuite découpé en paquets, représentant chacun par exemple 0,1 seconde de son ou d'image ; pour chaque paquet, on choisit une valeur numérique formant clef de paquet telle que la possession de la clef maîtresse d'un premier algorithme cryptographique ALG1 soit nécessaire pour calculer cette clef de paquet. A titre d'exemple, on associe à chaque paquet un indice incrémental et la clef de paquet est obtenue en chiffrant l'indice avec la clef maîtresse par un algorithme triple-DES.

e4) Chaque paquet est ensuite chiffré avec un second algorithme cryptographique ALG2 utilisant comme clef la clef de paquet (on notera que le flux de données pour le premier algorithme ALG1 est de l'ordre de 10^3 bps, très inférieur au flux de données du second algorithme ALG2, qui est celui ϕ à moyen débit des données comprimées).

Le flux chiffré résultant de l'étape e4 est ensuite diffusé, accompagné d'informations complémentaires nécessaires au calcul des clefs de paquet, dans cet exemple les indices de paquet. Il peut s'agir d'une diffusion à sens unique, du type satellite, cédérom ou DVD-ROM, ou à la demande, telle qu'une diffusion par câble, via Internet, par le réseau téléphonique commuté ou RNIS.

Bien entendu, cette diffusion s'accompagne de diverses opérations de vérification de l'intégrité de l'information transmise et de correction éventuelles d'erreurs, qui ne sont pas concernées par la présente invention.

On notera que le terme "diffusion" ne doit pas être entendu au sens technique strict (télédiffusion ou radiodiffusion, par voie hertzienne ou filaire) mais qu'il inclut également, par exemple, la diffusion d'informations par

distribution de supports physiques tels que cédéroms, DVDs, disquettes, etc., les enseignements de l'invention s'appliquant aussi bien au déchiffrement et à la décompression d'informations lues sur un support physique de cette nature.

On va maintenant décrire les étapes mises en œuvre du côté du récepteur.

Le récepteur ou décodeur comporte un microcircuit électronique sécurisé, c'est-à-dire protégé contre l'analyse et la duplication de son contenu, et contenant la clef maîtresse nécessaire au déchiffrement.

Les étapes successivement mises en œuvre sont les suivantes (on utilisera des références comprenant des indices homologues des étapes correspondantes mises en œuvre à l'émission) :

r3) Le microcircuit reçoit les informations nécessaires au calcul des clefs de paquet (dans le présent exemple, les indices de paquet) et applique le premier algorithme cryptographique ALG1 ; il communique les clefs de paquet ainsi calculées au reste du décodeur.

r4) Le décodeur déchiffre ensuite les paquets en utilisant le second algorithme cryptographique ALG2 et la clef de paquet correspondant, produisant un flux de données ϕ identique à celui résultant de l'étape e2, c'est-à-dire des données comprimées de moyen débit.

r2) Le décodeur décomprime ensuite ce flux de données ϕ, opération qui nécessite des moyens relativement limités par rapport à ceux mis en œuvre à l'étape e2, donnant ainsi un flux de données de grand débit Φ' comparable au flux Φ résultant de l'étape e1, mais non identique du fait des modifications liées au processus de compression/décompression.

r1) Le décodeur convertit ce flux de données Φ' de manière accessible aux sens humains, par exemple en commandant la vibration d'une membrane de haut-parleur ou la luminescence d'un tube cathodique ; typiquement cette étape r1 comporte tout d'abord une conversion numérique/analogique.

On notera que le système ici décrit est un système numérique, ce qui permet une forte compression à l'étape e2.

Le processus peut être également transposé à un système analogique, par exemple pour les systèmes de conception plus ancienne utilisant à

l'étape e2 un encodage analogique du type PAL, SECAM ou NTSC et pour e4 un chiffrement analogique du type permutation ou rotation de lignes ; le principe de fonctionnement est identique, quoique le flux résultant de l'étape r4 ne soit, dans ce cas, qu'approximativement identique au flux ϕ résultant de l'étape e2.

La technique que l'on vient d'exposer présente un certain nombre de points faibles qui la rendent vulnérable.

Même si l'on suppose que le microcircuit et le premier algorithme cryptographique ALG1 sont effectivement résistants, il reste diverses attaques possibles lorsque l'on souhaite enregistrer l'information sous une forme exploitable, à savoir :

1°) L'attaque du second algorithme ALG2, c'est-à-dire la reconstitution de l'étape r4 sans disposer du flux de données résultant de l'étape r3, par exemple en utilisant des redondances dans le flux de données résultant normalement de r4 ; la conception du second algorithme s'efforce de rendre cette opération difficile, mais on ne peut exclure une attaque réussie — impliquant de changer tous les décodeurs qui utilisent ce second algorithme ALG2.

2°) L'enregistrement, d'une part, du flux d'informations cryptées tel que diffusé (en entrée de r4) et, d'autre part (sur un décodeur équipé du microcircuit légitime), du flux des clefs de paquet, puis le décodage par un décodeur dénué du microcircuit légitime et recevant ces deux flux d'informations. Le volume de données représenté par les clefs de paquet étant très faible, ces informations peuvent par exemple être mises à disposition par radio ou sur Internet.

3°) L'enregistrement du flux d'informations déchiffrées résultant de l'étape r4, suivi de son exploitation ultérieure dans un dispositif appliquant r2 et r1. Cet enregistrement peut se faire :

- sur un décodeur équipé du microcircuit légitime, en récupérant les informations transitant de l'étage réalisant r4 vers celui réalisant r2 (les décodeurs les plus récents tentent d'éviter cette attaque en regroupant les étapes r4 et r2 dans un même circuit, où le flux en question est peu accessible).
- en reproduisant l'étape r4 dans un dispositif approprié, recevant d'une part le flux d'informations cryptées tel que diffusé,

d'autre part le flux des clefs de paquet issues d'un microcircuit légitime, le dispositif reproduisant le déchiffrement par l'algorithme rapide (cette attaque pouvant se combiner à la précédente).

4°) L'enregistrement du flux d'informations résultant de l'étape r2. Mais le débit à ce stade étant élevé, en particulier pour la vidéo, le fraudeur aura intérêt à recomprimer les données, c'est-à-dire appliquer une étape similaire à e2 ; on peut supposer que la difficulté technique de l'opération, ainsi que la perte de qualité résultante (perte d'autant plus importante que les moyens utilisés sont modestes) diminue l'attrait de la technique.

5°) L'enregistrement des signaux sous une forme dérivée de r2, par exemple une forme analogique intermédiaire utilisée dans r1. La réduction de qualité est alors nette ; de plus, on connaît divers moyens analogiques empêchant de faire une copie de qualité acceptable avec un enregistreur vidéo grand public.

L'invention s'efforce de remédier à ces inconvénients qui rendent le système vulnérable aux tentatives des fraudeurs.

Elle consiste essentiellement à intégrer dans le microcircuit de sécurité la totalité du déchiffrement (étapes r3 + r4 ci-dessus) et au moins la plus grande partie de la décompression (étape r2 ci-dessus), de sorte que le flux ϕ (de moyen débit) de données déchiffrées et comprimées ainsi que le flux des clefs de paquet ne soient pas présents hors du microcircuit et ne soient donc jamais accessibles.

On a illustré sur la figure 1 en traits tiretés les limites du microcircuit sécurisé, dans les deux variantes M, où ce microcircuit inclut la totalité des étages de décompression de l'étape r2, et M', où il ne met en œuvre qu'une partie de cette étape.

Dans ces conditions, l'attaque n° 1 (exposée plus haut) est rendue plus difficile, car l'algorithme cryptographique peut rester secret. De plus, si sa sécurité est compromise par un défaut de conception et qu'il doit être remplacé par un autre algorithme, il est possible de changer le seul microcircuit si ce dernier est amovible, sans modification du décodeur lui-même. Un avantage annexe est que l'on peut utiliser des algorithmes variant selon la zone de diffusion, voire faire évoluer l'algorithme de décom-

pression. Enfin, le boîtier du décodeur seul (c'est-à-dire sans son microcircuit sécurisé) ne contenant aucun algorithme cryptographique, n'est soumis à aucune réglementation particulière.

Les attaques n° 2 et n° 3 précitées sont rendues impossibles, puisque les flux de données intermédiaires nécessaires pour ces attaques restent internes au microcircuit.

Le système que l'on vient de décrire peut se présenter sous une forme simplifiée, avec les deux algorithmes de chiffrement ALG1 et ALG2 regroupés en un seul.

Dans ces conditions, les étapes côté émetteur seront :

e1) Production des signaux numériques (sans changement),

e2) Compression (sans changement),

e5) Chiffrement du flux ϕ des données par un procédé cryptographique utilisant une clef maîtresse.

Côté récepteur, le décodeur comprend un microcircuit électronique sécurisé qui contient la clef maîtresse. Les étapes mises en œuvre sont :

r5) Le microcircuit reçoit le flux de données résultant de e5 et le déchiffre, reconstituant (en l'absence d'erreur de transmission) le flux de données ϕ tel qu'il avant été produit à l'étape e2.

r2) Le *même* microcircuit (le fait qu'il s'agisse du même microcircuit, et non d'un autre circuit du décodeur, est une caractéristique essentielle de l'invention) décomprime ce flux de données ϕ, produisant un flux de données Φ', comparable à celui Φ résultant de l'étape e1 (les différences tenant au processus de compression/décompression). Ce flux Φ' est communiqué par le microcircuit au reste du décodeur.

r1) Conversion sous forme perceptible aux sens (sans changement).

Comme illustré figure 2, l'invention peut être mise en œuvre par un boîtier 10 assurant l'interfaçage entre, d'une part, des moyens 12 de réception hertzienne (typiquement une antenne ou un décodeur satellite), un réseau câblé 14, un lecteur de DVD-ROM 16, etc. et, d'autre part, un récepteur de télévision 18 ou une chaîne haute-fidélité 20. Le boîtier peut comprendre un mécanisme de sélection de programmes et/ou d'acheminement sélectif d'un programme à la demande.

Ce boîtier coopère avec un microcircuit sécurisé 22, par exemple le mi-

crocircuit d'une carte amovible 24 insérée dans une fente 26 du boîtier 10, l'ensemble boîtier 10 + microcircuit 22 constituant le "décodeur" mentionné plus haut.

L'information sélectionnée parvient, comprimée et chiffrée, du boîtier 10 au microcircuit 22, et celui-ci — s'il contient la clef appropriée et éventuellement si d'autres conditions sont remplies, par exemple le débit de points prépayés ou le télépaiement d'un abonnement ou de l'accès à un programme — la déchiffre et la décomprime, sans que la forme déchiffrée et comprimée ne soit accessible. Le flux décomprimé est délivré par le microcircuit 22 au boîtier 10 pour être appliqué, après les conversions appropriées au téléviseur 18 ou l'amplificateur de la chaîne 20.

Ce principe de base peut recevoir plusieurs perfectionnements.

Un *premier perfectionnement* vise à optimiser la connexion du microcircuit au boîtier, ainsi que la répartition entre microcircuit et boîtier des éléments intervenant dans le processus de décompression r2 et de conversion r1.

Tout d'abord, pour réduire au minimum le nombre de contacts, la liaison entre le microcircuit et le boîtier est avantageusement de type série.

Pour les flux de données, en particulier le flux Φ' de grand débit sortant de r2, on peut utiliser les contacts "RFU" ("réservé pour usage futur") de la norme ISO 7816-2.

La figure 3 montre la disposition des contacts d'une carte à microcircuit selon cette norme.

On notera que les contacts de masse GND, d'alimentation VCC, d'horloge CLK, de remise à zéro RST et d'entrée/sortie I/O gardent leurs fonctions habituelles, I/O servant pour les fonctions de supervision telles celles de l'étape r3 et/ou, par multiplexage, pour les flux de données plus lents, en particulier les flux entrant dans r5.

La synchronisation de ces flux de données série se fait par une boucle à verrouillage de phase intégrée au microcircuit, synchronisée sur un signal entrant dans le microcircuit tel que les données entrant dans r5 et/ou sur CLK.

On prévoit dans le code de données sortant du microcircuit un code de détection d'erreur et une inhibition de la restitution sonore ou visuelle lorsque le boîtier détecte une erreur dans ce flux, ceci pour prévenir des

bruits ou images indésirables, lorsque le microcircuit présente un mauvais contact avec le boîtier.

Par ailleurs, toujours dans ce perfectionnement visant à optimiser la connexion du microcircuit au boîtier, on peut déporter dans le boîtier les dernières étapes du processus de décompression r2, ceci afin de diminuer la complexité du microcircuit, en particulier la quantité de mémoire et la puissance de traitement nécessaires.

Dans le cas de signaux audio, on sait que les procédés de décompression comprennent dans la phase précédant la conversion numérique/analogique la génération et la combinaison de divers signaux dont les caractéristiques sont calculées par ailleurs, par exemple la génération et l'addition numérique de signaux tels que sinusoïde et/ou ondelette et/ou bruit dont la fréquence et/ou l'amplitude et/ou le spectre et/ou l'enveloppe sont paramétrés. On peut alors prévoir que la commande (paramétrage) de ces générateurs soit réalisée par le microcircuit, mais que la génération et la combinaison proprement dites soient réalisées dans le boîtier, l'essentiel de la puissance de calcul étant ainsi déporté dans ce boîtier.

En vidéo, les procédés de décompression comprennent dans la phase finale de génération du signal décodé la recopie d'informations provenant de lignes et trames d'images précédentes et/ou le remplissage de zones. On peut alors prévoir que le boîtier stockera ces informations et réalisera les copies et le remplissage, mais selon des paramètres produits par le microcircuit.

A contrario, si l'on dispose encore dans le microcircuit d'une puissance de calcul suffisante, on peut intégrer dans celui-ci non seulement la décompression r2, mais également les premières phases du processus de conversion r1, afin d'augmenter le débit binaire de l'information sortant du microcircuit et rendre son stockage plus difficile, ce qui permet de lutter plus efficacement, dans une certaine mesure, contre l'attaque n° 4 précitée. En particulier, pour de l'audio, on peut intégrer dans le microcircuit le traitement numérique tel que la modification du nombre de bits de l'échantillonnage et/ou le filtrage numérique, permettant de diminuer la complexité du filtre analogique placé en aval du convertisseur numérique/analogique du boîtier.

Un *deuxième perfectionnement* consiste à réaliser chacune des étapes e5

et r5 en deux étapes respectives e3 + e4 et r3 + r4 mettant en jeu deux algorithmes distincts, ce qui est justifié cryptographiquement parlant, dans le but de réaliser l'opération avec un bon compromis complexité/coût.

Un *troisième perfectionnement* consiste à prévoir un mécanisme supplémentaire destiné à tarifer l'utilisation du système.

On prévoit à cet effet dans le microcircuit un moyen de conditionner la production des informations déchiffrées à la réalisation préalable d'un payement, moyen opérant en traitant le contenu d'une mémoire contenant les droits du possesseur du microcircuit. Cette mémoire peut être située dans le microcircuit lui-même, ou bien dans le boîtier, ou encore chez le diffuseur d'informations.

Ces droits évoluent en fonction de l'usage qui est fait du système ; par exemple une zone de crédit de cette mémoire est débitée à la première diffusion de l'information, par exemple la première audition d'un morceau de musique, et l'identifiant de ce morceau est stocké dans cette mémoire, permettant à l'utilisateur qui souhaite réécouter ultérieurement le même morceau de le faire sans débit, ou à débit réduit. Certaines opérations sont inhibées lorsque le crédit tombe à zéro. Des moyens de rechargement sont prévus par ailleurs.

Si elle est chez le diffuseur, la mémoire peut être subdivisée en zones correspondant chacune à un microcircuit donné, la zone adéquate étant sélectionnée à partir d'un identifiant du microcircuit contenu dans une mémoire de celui-ci.

Outre l'enregistrement dans la mémoire d'un identifiant du morceau, l'achat des droits peut être matérialisé par le stockage dans la mémoire du microcircuit de la clef et/ou de l'algorithme de déchiffrement de ce morceau ; cette mesure permet d'éviter d'avoir une clef et/ou un algorithme universels valables pour tous les morceaux.

On prévoira qu'aux données comprimées et chiffrées est ajoutée une information d'identification/tarification exploitée par le microcircuit pour déterminer quelle clef et/ou algorithme de déchiffrement et/ou quelle tarification est à appliquer au flux d'information chiffré. À une étape e6 (par exemple postérieure à e5), cette information d'identification/tarification est ajoutée au flux de données ; et à une étape r6 (par exemple préalable à r5), cet identifiant est extrait et exploité par le microcircuit pour déterminer

quelle clef et/ou quel algorithme utiliser à l'étape 5, et/ou quelle tarification appliquer (par exemple si les droits de déchiffrement par le microcircuit sont acquis définitivement, ou font l'objet d'un payement à chaque utilisation, et à quel tarif).

Pour protéger la partie tarification de cette information contre les altérations intentionnelles, on peut utiliser une méthode cryptographique, par exemple l'ajout d'une signature électronique des données incluant la tarification et vérifiée par le microcircuit, ou en insérant cette information de tarification avant le chiffrement, de sorte que son altération rapide rende inexploitable le reste des données.

Un *quatrième perfectionnement* consiste à associer un enregistreur au système de l'invention.

A cet effet, le boîtier 10 peut contenir un dispositif d'enregistrement de l'information (ou comprendre des moyens de connexion à un tel dispositif), permettant une utilisation ultérieure sans qu'il soit nécessaire d'acheminer l'information par la voie de diffusion.

L'information peut être enregistrée sous forme encore comprimée et chiffrée ; elle sera déchiffrée et décomprimée à la relecture, qui nécessitera donc la présence du microcircuit (cette prestation pouvant éventuellement être accompagnée d'un paiement). L'enregistrement peut également avoir lieu de façon concomitante à la première utilisation.

Ces dispositifs d'enregistrement peuvent par exemple prendre la forme d'une mémoire à semiconducteurs, d'un disque dur 28, d'une bande magnétique 30 de type DAT, d'un disque 32 magnéto-optique ou de type WORM optique ou DVD-RAM, etc., si l'on souhaite un enregistrement numérique direct. En variante ou en complément, le boîtier 10 peut également comporter des moyens de conversion numérique/analogique pour l'enregistrement et de conversion analogique/numérique pour la lecture dans le cas d'un enregistrement analogique, typiquement sur un magnétoscope VHS.

REVENDICATIONS

1. Un dispositif décodeur d'informations chiffrées et comprimées, notamment d'informations vidéo, audio ou de texte, du type comprenant un boîtier (10) coopérant avec un microcircuit sécurisé (22) comportant une mémoire et un processeur protégés à l'encontre des tentatives d'analyse et de lecture et de recopie des informations conservées dans ce microcircuit, ce dispositif décodeur comportant :

- des moyens de réception en entrée de données chiffrées et comprimées,
- des moyens de déchiffrement (r5 ; r3, r4) des données ainsi reçues,
- des moyens de décompression (r2) des données ainsi déchiffrées, et
- des moyens de délivrance (r1) en sortie, sous une forme décodée exploitable par un utilisateur, des données déchiffrées et décomprimées,

dispositif caractérisé en ce que le microcircuit sécurisé incorpore l'ensemble des moyens de déchiffrement (r5 ; r3, r4) et au moins une partie des moyens de décompression (r2), le flux (ϕ) de données déchiffrées et comprimées délivré par les moyens de déchiffrement aux moyens de décompression n'étant pas accessible depuis l'extérieur du microcircuit sécurisé.

2. Le dispositif de la revendication 1, dans lequel le microcircuit sécurisé (22) est celui d'une carte à microcircuit (24) distincte du boîtier, ce dernier comportant des moyens de connexion permettant d'y coupler la carte à microcircuit.

3. Le dispositif de l'une des revendications 1 et 2, dans lequel le microcircuit sécurisé est un microcircuit interne au boîtier.

4. Le dispositif de l'une des revendications 2 et 3, dans lequel la liaison entre le microcircuit et le boîtier est une liaison de type série.

5. Le dispositif de la revendication 4, dans lequel le flux de données déchiffrées et partiellement ou totalement décompressées est délivré par le microcircuit sur au moins l'un des contacts RFU selon ISO 7816-2.

6. Le dispositif de l'une des revendications 1 à 5, dans lequel le boîtier comporte une partie des moyens de décompression (r2), cette partie incluant des circuits propres à délivrer les données décomprimées en réponse à des commandes délivrées par le microcircuit sécurisé.

7. Le dispositif de l'une des revendications 1 à 6, dans lequel le microcircuit sécurisé inclut en outre une partie des moyens de délivrance (r1) en sortie des données sous une forme décodée exploitable, cette partie incluant notamment des moyens de traitement ou de filtrage numériques.

8. Le dispositif de l'une des revendications 1 à 7, dans lequel les données reçues en entrée le sont sous forme de paquets accompagnés de données associées, et les moyens de déchiffrement opèrent par mise en œuvre d'un premier algorithme (ALG1) permettant le calcul de clefs de paquet à partir desdites informations associées, et d'un deuxième algorithme (ALG2) reconstituant un flux (ϕ) d'informations déchiffrées à partir des paquets et des clefs de paquet calculés par le premier algorithme.

9. Le dispositif de l'une des revendications 1 à 8, comprenant des moyens de paiement conditionnant la délivrance en sortie des données sous une forme décodée exploitable à la vérification, par le microcircuit, de la réalisation préalable d'un payement en fonction d'informations tarifaires associées contenues dans une mémoire.

10. Le dispositif de la revendication 9, dans lequel les informations tarifaires comportent une information d'identification d'utilisateur contenue dans une mémoire du microcircuit sécurisé.

11. Le dispositif de l'une des revendications 1 à 10, comprenant des moyens d'enregistrement ou des moyens de couplage à des moyens d'enregistrement (38, 30, 32).

12. Le dispositif de la revendication 11, dans lequel les données délivrées aux moyens d'enregistrement sont des données comprimées et chiffrées.

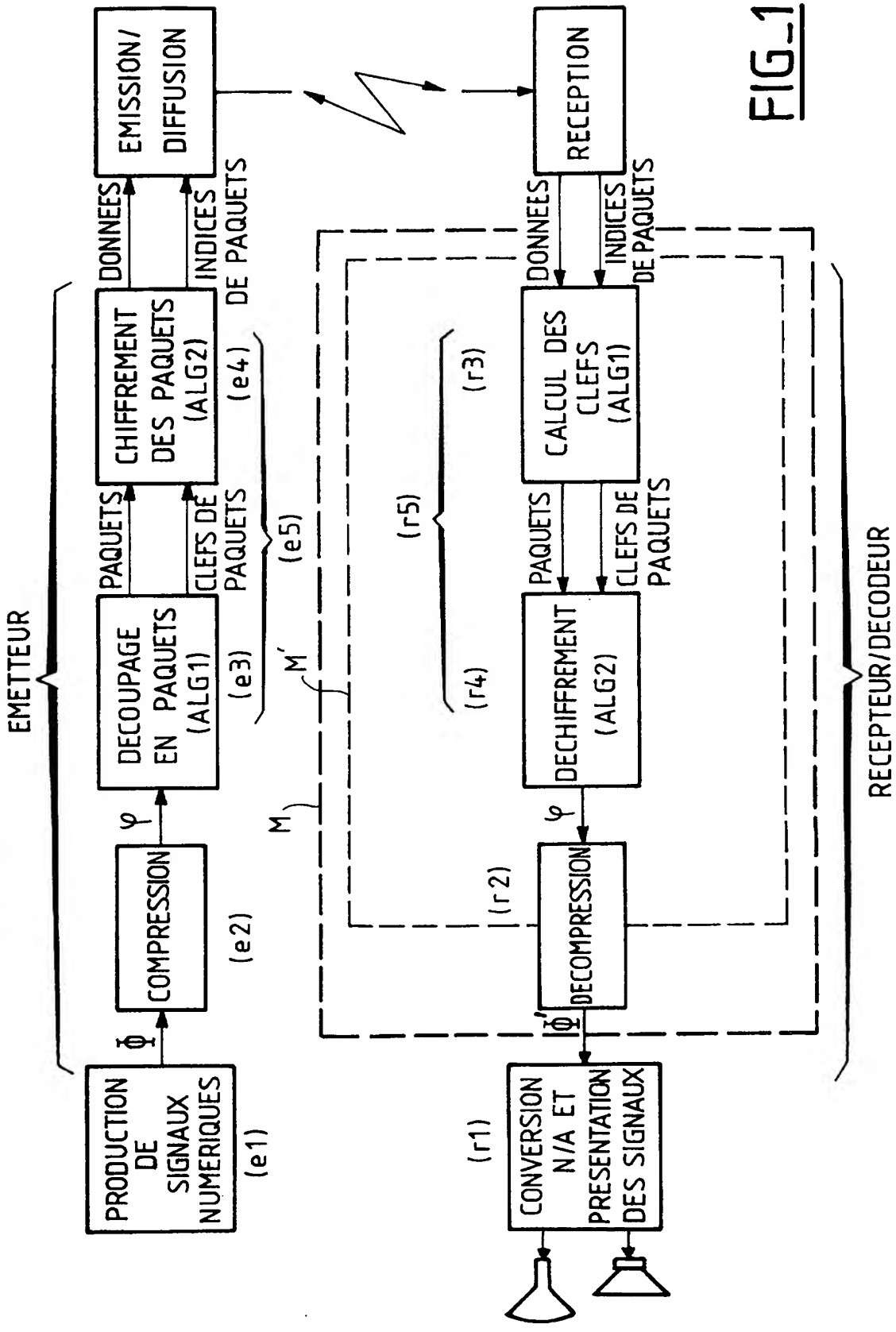

EMETTEUR
PRODUCTION DE SIGNAUX NUMERIQUES
(e1)
COMPRESSION
(e2)
DECOUPAGE EN PAQUETS (ALG1)
(e3)
CHIFFREMENT DES PAQUETS (ALG2)
(e4)
EMISSION/ DIFFUSION
DONNEES
INDICES DE PAQUETS
PAQUETS
CLEFS DE PAQUETS
(e5)
M
M'
(r1)
CONVERSION N/A ET PRESENTATION DES SIGNAUX
(r2)
DECOMPRESSION
(r3)
CALCUL DES CLEFS (ALG1)
(r4)
DECHIFFREMENT (ALG2)
(r5)
RECEPTION
RECEPTEUR/DECODEUR

FIG_1

FIG_2

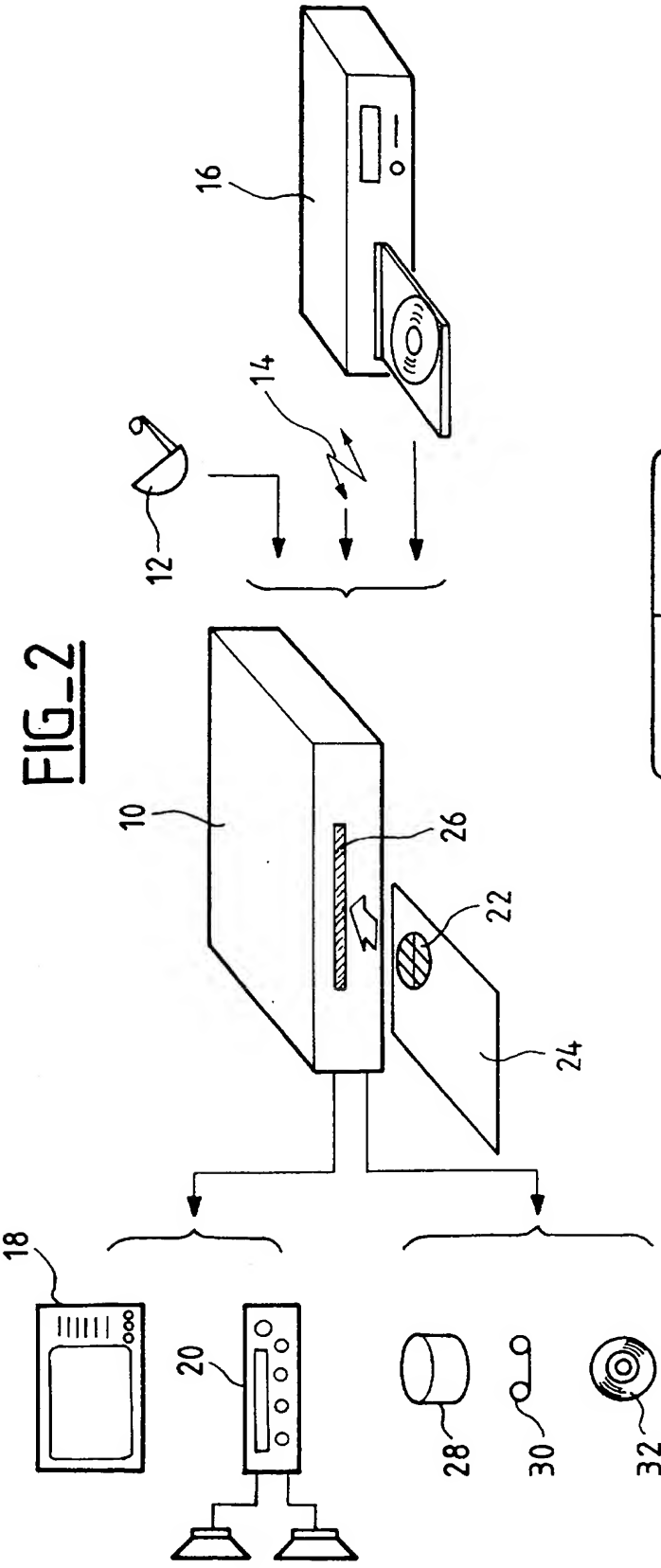
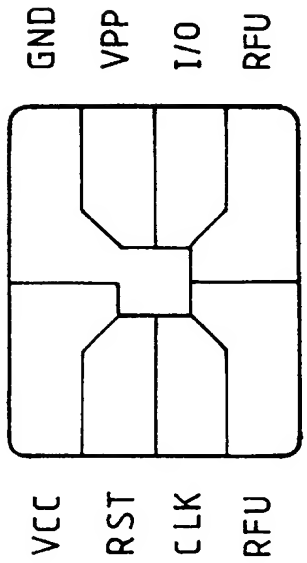


FIG_3



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2786973

N° d'enregistrement national

FA 569478
FR 9815377

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	PEYRET P ET AL: "SMART CARDS PROVIDE VERY HIGH SECURITY AND FLEXIBILITY IN SUBSCRIBERS MANAGEMENT" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 36, no. 3, 1 août 1990, pages 744-752, XP000162915 New York, NY, US * page 745, colonne de gauche, ligne 4 - page 748, colonne de droite, ligne 30 * * page 749, colonne de droite, ligne 1 - ligne 24 *	1-10	
X	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 juillet 1996	1-3,6-12	
Y	* page 2, colonne 1, ligne 32 - colonne 2, ligne 51 * * page 3, colonne 3, ligne 57 - page 5, colonne 7, ligne 8 * * figures 1-4 *	4,5	
X	EP 0 714 204 A (LG ELECTRONICS INC) 29 mai 1996 * page 2, ligne 5 - ligne 8 * * page 6, ligne 1 - page 11, ligne 2 * * figures 7-20 *	1-3,6-12	DOMAINES TECHNIQUES RECHERCHES (Int.CL.6) H04N
Y	EP 0 453 737 A (GAO GES AUTOMATION ORG) 30 octobre 1991 * page 2, colonne 1, ligne 17 - ligne 48 * * page 4, colonne 5, ligne 56 - colonne 6, ligne 51 *	4,5	

Date d'achèvement de la recherche	Examinateur
2 juillet 1999	Van der Zaal, R

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)